Fortify ソフトウェア セキュリティ コンテンツ

2024 年更新版 2
2024 年 6 月 28 日

OpenText Fortify Software Security Research について

Fortify Software Security Research チームの役割は、最新のセキュリティ調査をもとに OpenText™ Fortify Static Code Analyzer や OpenText™ Fortify WebInspect を含む Fortify 製品ポートフォリオを強化するセキュリティ インテリジェンスをもたらすことです。現在、Fortify ソフトウェア セキュリティ コンテンツは、33 以上の言語における 1,660 もの脆弱性カテゴリをサポートし、100 万を超える API を網羅しています。

Copyright © 2024 Open Text.All rights reserved.商標は Open Text が所有。

Fortify Software Security Research (SSR) は、Fortify Secure Coding Rulepacks (英語版、バージョン 2024.2.0)、Fortify WebInspect SecureBase (SmartUpdate で利用可能)、および Fortify Premium Content への更新をまもなくリリースいたします。

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

このリリースにより、Fortify Secure Coding Rulepacks は 33 以上の言語で脆弱性に関する 1,435 の固有のカテゴリを検出し、100 万を超える個々の API を網羅します。今回のリリースで追加された主な機能は次のとおりです。

改善された Node.js のサポート (サポートされているバージョン: 21.x)[1]

Node.js は、開発者がサーバー、Web アプリケーション、コマンド ライン ツールなどを作成できるクロスプラットフォームの JavaScript ランタイム環境です。このリリースには、Node.js 21.x の次のモジュールに対する Node.js サポートの重要な更新が含まれています。

- async_hooks
- buffer
- child_process
- crypto
- dgram
- dns
- fs
- http
- https
- net
- os
- path
- process
- punycode
- querystring
- stream
- string_decoder
- timers
- tls
- url
- util
- v8
- vm
- worker_threads
- zlib

これらの更新により、次の脆弱性カテゴリの問題検出が改善されます。

- Command Injection
- Dynamic Code Evaluation: Code Injection
- Header Manipulation

[1] Fortify Static Code Analyzer 24.2 以降が必要です。

- Insecure Transport: Weak SSL Cipher
- Insecure Transport: Weak SSL Protocol
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- System Information Leak
- System Information Leak: External

また、Node.js アプリケーション用に、このリリースでは次の脆弱性カテゴリが導入されています。

- DNS Spoofing
- Dynamic Code Evaluation: Script Injection
- Insecure Transport: Insufficient Diffie Hellman Strength
- Key Management: Empty HMAC Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Empty PBE Salt
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Hash: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Stream Cipher

改善された Java のサポート (サポートされているバージョン: 21)

Java 21 は、Java プラットフォームの最新の長期サポート (LTS) バージョンです。既存の API の機能強化だけでなく、多数の新機能も含まれています。特に重要なものは次のとおりです。外部関数とメモリ、シーケンス コレクション、キーのカプセル化、仮想スレッド、構造化並行性、無名変数、スコープ値。これらの機能の一部はまだプレビュー状態ですが、対象範囲を含めるのに十分なほど成熟していると考えられます。更新されたカテゴリは次のとおりです。

- Process Control
- Unreleased Resource
- Weak Encryption
- Weak Cryptographic Hash

さらに、次の新しいカテゴリがサポートされています。

- Restricted Method
- Weak Cryptographic Signature: XML Signature Secure Validation Disabled

改善された MyBatis のサポート (サポートされているバージョン: 3.5.x)

MyBatis は、リレーショナル データベース内のオブジェクトと、オブジェクト指向アプリケーション内のオブジェクトを結合するために使用される SQL マッパーです。このフレームワークは、XML 記述子またはコード注釈を使用してストアド プロシージャと SQL ステートメントを組み合わせ、開発プロセスとデータベース通信を容易にします。MyBatis のサポートがバージョン 3.5.16 に引き上げられました。改善点には、次の脆弱性カテゴリのサポートの更新が含まれます。

- Dynamic Code Evaluation: Unsafe Deserialization
- SQL Injection
- System Information Leak
- Unreleased Resource: Database
- Unsafe Reflection

MyBatis-Plus の初期サポート (サポートされているバージョン: 3.5.x)

MyBatis-Plus は既存の MyBatis フレームワークを基盤として構築されており、元のフレームワークにある機能を超える便利で効率的なすぐに使える機能を提供することによって開発を簡素化します。MyBatis-Plus 3.5.x の初期サポートが提供されます。初期カテゴリ サポートは、*SQL Injection* に対して提供されます。

人工知能 (AI) および機械学習 (ML) モデルに起因するリスクの検出

生成 AI と大規模言語モデル (LLM) の使用により、ソフトウェア業界のソリューション領域が急速に変化しており、新たなリスクが生じています。このリリースでは、OpenAI API (Python および JavaScript)、TensorFlow (Python)、または Anthropic Claude (Python および JavaScript) を使用するプロジェクトの対象範囲が拡大しました。サポートは、AI/ML モデル API からの応答の暗黙的な信頼に起因する脆弱性を検出するだけでなく、次の機能も検出します。

改善された OpenAI のサポート (サポートされているバージョン: 1.14.x [Python]、4.33.x [JavaScript])

Python、TypeScript、JavaScript 用の OpenAI ライブラリは、高度な AI 機能をさまざまなアプリケーションに統合するための包括的なツールを提供します。これらのライブラリは、自然言語処理、テキスト生成、会話型 AI など、幅広い機能をサポートしています。直感的でユーザーフレンドリーな API により、開発者は OpenAI の最先端の AI モデルをプロジェクトにシームレスに埋め込むことができ、Python、TypeScript、JavaScript 環境全体でインタラクティブ性とインテリジェンスを強化できます。サポートの改善により、*Cross-Site Scripting: AI* の対象範囲が拡大され、2 つの新しい脆弱性カテゴリが追加されました。

- Cross-Site Scripting: DOM AI
- Prompt Injection

TensorFlow (サポートされているバージョン: 2.16.x)

Google による先進的なオープンソース機械学習フレームワークである TensorFlow は、機械学習モデルを作成および展開するための強力なツール スイートを提供します。組み込みライブラリとトレーニング済みモデルにより、ディープ ラーニング アプリケーションの構築が簡素化されます。TensorFlow は、研究プロトタイプから大規模な本番環境システムまで、多様なプロジェクトに合わせて拡張できます。初期の対象範囲には次のカテゴリのサポートが含まれます。

- Path Manipulation
- Privacy Violation
- System Information Leak: Internal

さらに、サポートでは新しい脆弱性カテゴリが追加されました。

- Dynamic Code Evaluation: Unsafe TensorFlow Deserialization

Anthropic Claude SDK (サポートされているバージョン: 0.21.3 [Python]、0.20.5 [JavaScript])

Python および JavaScript 用の Anthropic Claude ライブラリは、洗練された AI 言語モデルである Claude をアプリケーションに統合するための包括的なツールを提供します。初期サポートには、*Cross-Site Scripting: AI* の対象範囲が拡大され、2 つの新しい脆弱性カテゴリが追加されました。

- Cross-Site Scripting: DOM AI
- Prompt Injection

改善された Django のサポート (サポートされているバージョン: 5.0.x)

Django は、安全かつ迅速な Web 開発を促進するように設計され、Python で記述された Web フレームワークです。開発の速度と安全性は、コードの構築と生成を使用して定型コードを大幅に縮小する、フレームワークの高度な抽象化によって実現されます。このリリースでは、既存の Django の対象範囲を更新し、バージョン 5.0.x までのリリースをサポートしています。

これらの更新により、次の脆弱性カテゴリの問題検出が改善されます。

- Access Control: Database
- Cookie Security: CSRF Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set on CSRF Cookie
- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Cross-Frame Scripting
- Cross-Site Request Forgery
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- Insecure Transport
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Privacy Violation: BREACH
- SQL Injection

Paramiko の初期サポート (サポートされているバージョン: 3.4.x)

Paramiko は、SSH 経由でマシンに接続するための Python ライブラリです。Paramiko は、開発者から暗号化メソッドを抽象化する一連の機能を提供します。これにより、ソケット プログラミングに似た高レベルの機能が提供され、開発者は SSH 接続のマイクロ管理構成のための低レベルのメソッドにアクセスできるようになります。初期サポートでは、次の脆弱性カテゴリを対象としています。

- Command Injection
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Cipher
- Password Management: Hardcoded Password
- SSH Misconfiguration: Missing Authentication

改善された PHP のサポート (サポートされているバージョン: 8.3)

PHP は広く使用されている汎用スクリプト言語であり、Web 開発に最もよく使用されます。このリリースでは、PHP のサポートがバージョン 8.3 までを対象とするように更新されました。特に、このリリースには、次の拡張機能のサポートの改善が含まれています。

- DOM (サポートされているバージョン: 8.3)

  PHP の DOM 拡張機能により、ドキュメント オブジェクト モデルを使用して PHP で XML および HTML ドキュメントを操作できるようになります。このライブラリの拡張サポートには、DOM 操作のデータフロー サポートの改善と、*Setting Manipulation* 脆弱性を識別するための追加の対象範囲が含まれます。

- JSON (サポートされているバージョン: 8.3)

  PHP の JSON 拡張機能により、PHP ライセンスに基づいて作成されライセンスされた JSON パーサーを使用できるようになります。この拡張機能の初期サポートには、拡張機能の機能に対するデータフロー サポートが含まれます。

- OpenSSL (サポートされているバージョン: 8.3)

  PHP の OpenSSL 拡張機能は、さまざまな暗号化操作のために OpenSSL ライブラリの機能を実装します。このライブラリの拡張サポートには、暗号化キー ペアのデータフロー サポートの改善が含まれています。

- Simdjson (サポートされているバージョン: 8.3)

  PHP の Simdjson 拡張機能は、simdjson プロジェクトの PHP 固有のバインディングを実装し、高速な JSON デコードを実現します。初期サポートには、PHP の次の新しいカテゴリが含まれます。

  - JSON Path Manipulation

改善された iOS のサポート (サポートされているバージョン: 17)[2]

Apple の iOS SDK と iPadOS SDK は、開発者が Apple の iPhone および iPad デバイス用のモバイル アプリケーションを構築できるようにする一連のフレームワークを備えています。このリリースには、Swift および Objective-C に対する iOS SDK サポートのインクリメンタルな更新が含まれています。新しいルールと更新されたルールにより、iOS 17 での次のフレームワークの API 適用範囲が拡張されます。

- CryptoKit

[2] iOS 17 API には Xcode 15 以降が必要であり、さらに Fortify Static Code Analyzer 23.2 以降が必要です。ただし、Source Code Analyzer 23.2 を使用して iOS 17 API を使用するアプリをビルドすると、コンパイラの警告が表示される場合があります。有効なコンパイルとスキャンを確実に実行するには、Fortify Static Code Analyzer 24.2 以降を使用することをお勧めします。

- Foundation
- Network
- os
- System
- SwiftUI
- UIKit

これらの更新により、次の脆弱性カテゴリの問題検出が改善されます。

- Insecure Transport
- Path Manipulation
- Privacy Violation
- Privacy Violation: Health Information
- System Information Leak: External
- System Information Leak: Internal
- Unreleased Resource: Synchronization
- Unsafe Reflection
- Weak Cryptographic Hash
- Weak Cryptographic Hash: User-Controlled Salt
- Weak Encryption: User-Controlled Key Size

改善された MISRA C 2012 のサポート

MISRA は、ソフトウェアに高い整合性や信頼性が求められる安全性が重要な環境で使用されるアプリケーション開発のためのさまざまな標準を作成および維持する標準化団体です。このリリースには、MISRA C 2012 標準の 2 つの必須ガイドライン ルールに厳密に対応する 2 つの新しいカテゴリのサポートが含まれています。

- Undefined Behavior: File Pointer Dereference
- Undefined Behavior: File Pointer Use After Close

パスワード正規表現プロパティの更新

Fortify Static Code Analyzer バージョン 23.1 で導入されたパスワード正規表現プロパティは、Fortify ルールがさまざまな言語のパスワード識別子とどのように一致するかを指定する正規表現を含むカスタマイズ可能なプロパティです。このリリースでは、com.fortify.sca.rules.password_regex.global プロパティのデフォルト値を拡張し、「secret」という単語を含むパスワード識別子を認識するようになりました。さらに、動的に生成された JSON 文字列を解析する際にパスワード正規表現プロパティを利用するための新しいルールが追加されました。その結果、お客様は言語を問わず、次のカテゴリでの検出の改善が期待できます。

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Privacy Violation

改善された Golang のサポート (サポートされているバージョン: 1.21 まで)

Go (Golang とも呼ばれる) は、Google で作成されたコンパイル型の静的型付けプログラミング言語です。シンプルさ、効率性、並行処理の強力なサポートで知られており、スケーラブルな Web サービス、データ パイプライン、分散システムの構築に最適です。このリリースには、*Unreleased Resource* 脆弱性の検出が含まれており、GORM v2 を使用するプロジェクトに対する新たな *SQL Injection* 検出が導入されました。

WordPress API の改善 (サポートされているバージョン: 6.5 まで) (API 数: 2)

WordPress アプリケーション プログラミング インターフェイス (API) は、複数の API セクション/トピックに分割することができ、各セクション/トピックでは、特定の機能セットに関連する機能とその使用方法を対象としています。これらは一緒になって、WordPress プロジェクト全体によって作成されたプラグイン/テーマ/アドオン インターフェイスである WordPress API と呼ばれるものを形成します。このリリースでは、次の API の問題を特定するための初期サポートが追加されました。

- REST API
- Shortcode API

その他の正誤情報

このリリースでは、誤検知の数を減らし、一貫性を確保するためにリファクタリングを行い、お客様の側で問題をより深く調査いただけるようにするため、継続的に力を注いできました。お客様は、以下に関連して報告された問題の変化を確認することもできます。

誤検知の削減および検出機能に関するその他の改善点

このリリースでは、誤検知を排除する取り組みが引き続き行われています。誤検知がさらに減っており、以下の分野で著しい改善が見られることを実感いただけるはずです。

- *ASP.NET MVC Bad Practices: Optional Submodel With Required Property* - ASP.NET アプリケーションの誤検知を削減
- *Insecure Transport: Mail Transmission* - Java アプリケーションでの誤検知を削減
- *Password Management: Hardcoded Password* - JSON/YAML ファイルでの誤検知を削減
- *Unreleased Resource: Streams* - Java アプリケーションでの誤検知を削減
- *Password Management: Hardcoded Password* - Python アプリケーションで辞書型に関連する新しい問題を検出
- *Password Management: Hardcoded Password* - ASP.NET アプリケーションで補間された文字列に関連する新しい問題を検出
- 組み込みの JDK システム プロパティから発生する多くの誤検知を削除

カテゴリ名の変更

脆弱性カテゴリの名前が変更された場合、以前のスキャンの分析結果を新しいスキャンとマージすると、カテゴリが追加または削除される場合があります。

整合性向上のため、次の 3 件のカテゴリの名前を変更しました。

2024 R1 カテゴリ名	2024 R2 カテゴリ名
Access Control: gRPC Authentication Bypass	Access Control: gRPC Fail Open
AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS CloudFormation Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key
AWS Terraform Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS Terraform Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key

DISA Control Correlation Identifier (CCI) バージョン 2

米国国防情報システム局 (DISA) CCI は、一連の標準識別子と単一の実行可能なステートメントを組み合わせて提供することで、高レベルと低レベルのサイバーセキュリティ ガイダンスの間のギャップを埋めるドキュメントです。DISA のアプリケーション セキュリティおよび開発の STIG は DISA CCI に密接にマッピングされており、単一の STIG コントロールが 1 つ以上の CCI に適用される場合があります。このリリースでは、マッピングされた CCI が、以前のリリースでの Fortify Taxonomy に対する STIG マッピングの最近の更新と同等になります。

NIST Special Publication 800-53 リビジョン 4 および 5

National Institute of Standards and Technology (NIST) Special Publication 800-53 は、情報システムのセキュリティとプライバシー制御のカタログを提供する文書であり、サイバーセキュリティ分野全体でシステムのセキュリティ保護方法に関するガイダンスとして活用できます。NIST Special Publication 800-53 は DISA CCI に密接にマッピングされており、単一の CCI が 1 つ以上の NIST 800-53 コントロールに適用される場合があります。このリリースでは、マッピングされた NIST 800-53 コントロールが、Fortify Taxonomy に対する DISA CCI マッピングの最近の更新と同等になります。

OWASP Mobile Top 10 2023

以前に発表したように、Fortify Software Security Content のこのリリースでは、OWASP Mobile Top 10 2023 マッピングは廃止され、更新された OWASP Mobile Top 10 2024 のみが残りました。

Software Security Content のリリースを OpenText のバージョン管理と合わせる

次のリリースには、セキュリティ コンテンツのバージョン管理の変更が含まれる予定です。これは、「2024 Update 2」という命名規則に従う OpenText Fortify Software Security Content の最後のアップデート リリースになります。OpenText のバージョン管理標準に合わせて、リリースは毎年四半期ごとに 1 回スケジュールされ、年と四半期に応じて番号が付けられます。したがって、OpenText™ Fortify™ Software Security Content の次のリリースは 24.4 となり、2024 年の第 4 四半期の最初の月にリリースされることを示します。

Fortify SecureBase [Fortify WebInspect]

SmartUpdate を使用してすぐに入手できる以下の更新を実行すると、Fortify SecureBase で、お客様をガイドするポリシーと組み合わせて数千の脆弱性のチェックを行うことができます。

脆弱性のサポート

Denial of Service: GraphQL

API 用の GraphQL クエリ言語は、既存のデータをクエリするためのランタイムを提供します。GraphQL スキーマは、データ オブジェクト、そのフィールドとタイプ、および他のデータ オブジェクトとの関係で構成されるモデルです。異なるデータ オブジェクト間の参照によってサイクルが作成されることがあります。攻撃者は、悪意のあるネストされた高コストな循環クエリを作成してサービス拒否 (DoS) を引き起こし、CPU とメモリの過剰な使用を引き起こす可能性があります。このリリースには、GraphQL スキーマ内の循環参照を検出するためのチェックが含まれています。

Access Control: Authorization Bypass (CVE-2024-27198)

CVE-2024-27198 は JetBrains ソフトウェアの重大な脆弱性として識別されており、重大なセキュリティ上の脅威となります。この脆弱性は、認証メカニズムが不十分であることに関連するリスクを浮き彫りにしており、認証されていない攻撃者が、影響を受けたシステムの管理制御権を取得できる可能性があります。最新リリースには、対象のサーバー上でこの脆弱性を検出するためのチェックが含まれています。

Directory Traversal (CVE-2024-27199)

JetBrains TeamCity On-Premises サーバー バージョン 2023.11.4 より前のバージョンには、CVE-2024-27199 として識別されるパス トラバーサルの欠陥に対する脆弱性があります。攻撃者はこの欠陥を利用して認証制御を回避し、システムの整合性と機密性を著しく脅かす可能性があります。最新リリースには、対象のサーバー上でこの脆弱性を検出するためのチェックが含まれています。

Dynamic Code Evaluation: Unsafe Deserialization (CVE-2023-26360)

Adobe ColdFusion バージョン 2018 Update 15 以前、および 2021 Update 5 以前では、CVE-2023-26360 で識別される Dynamic Code Evaluation 脆弱性の影響を受けます。この脆弱性により、現在のユーザーのコンテキストで任意のコードが実行される可能性があります。この問題を悪用するにはユーザーの操作は必要ありません。このリリースには、対象のサーバー上でこの脆弱性を検出するためのチェックが含まれています。

Insecure Deployment: Unpatched Application (CVE-2024-32962)

CVE-2024-32962 は、Node.js の XML デジタル署名および暗号化ライブラリである xml-crypto に関連する重大な脆弱性です。この脆弱性はバージョン 4.0.0 で発生し、バージョン 6.0.0 で解決されました。この脆弱性は、影響を受けたバージョンではデフォルト構成で署名者の認証がチェックされないために発生します。攻撃者は、XML ドキュメントを改変し、既存の署名を不正なプライベートキーで生成された署名に置き換えて、対応する証明書を <KeyInfo/> 要素に添付することでこれを悪用することができます。このリリースには、影響を受けた xml-crypto バージョンを使用するターゲットサーバーでこの脆弱性を検出するためのチェックが含まれています。

その他の正誤情報

このリリースでは、誤検知の数を減らし、お客様の側で問題をより深く調査いただけるようにするため、継続的に力を注いできました。以下の分野に関連して報告された内容にも、問題の変化を実感いただけるはずです。

Insecure Deployment: OpenSSL

このリリースでは、誤検知を減らし、結果の精度を上げるため、OpenSSL ChangeCipherSpec Man-in-the-Middle (MitM) のチェックが改善されています。

Fortify Premium Content

リサーチ チームは、コア セキュリティ インテリジェンス製品以外の各種リソースの構築、拡張、保守管理を行います。

Fortify Taxonomy: ソフトウェア セキュリティ エラー

新たに追加されたカテゴリのサポートに関する説明が記載されている Fortify Taxonomy サイトは、https://vulncat.fortify.com にあります。

カスタマー サポートへの問い合わせ

OpenText Fortify
https://softwaresupport.softwaregrp.com/
+1 (800) 509-1800

SSR へのお問い合わせ

Alexander M. Hoole
Software Security Research、シニア マネージャー
OpenText Fortify
hoole@opentext.com
+1 (650) 427-9973

Peter Blay
Software Security Research、マネージャー
OpenText Fortify
pblay@opentext.com
+1 (669) 309-1634

© Copyright 2024 Open Text or one of its affiliates.The information contained herein is subject to change without notice.The only warranties for Open Text products and services are set forth in the express warranty statements accompanying such products and services.Nothing herein should be construed as constituting an additional warranty.Open Text shall not be liable for technical or editorial errors or omissions contained herein.